What is claimed is:

[c1] 1. A method comprising

requesting a first token to unseal a sealed first portion of a multi-token sealed object to obtain a first portion of the multi-token sealed object,

requesting a second token to unseal a sealed second portion of a multi-token sealed object to obtain a second portion of the multi-token sealed object, and

using the first portion and the second portion to obtain an object from the multi-token sealed object.

[c2] 2. The method of claim 1 further comprising obtaining the object of the multi-token sealed object by using the first portion as a key to decrypt the second portion .

[c3] 3. The method of claim 1 further comprising

receiving a key in response to the first token unsealing the sealed first portion,

receiving an encrypted object in response to the second token unsealing the second portion, and

obtaining the object of the multi-token sealed object by using the key to decrypt the encrypted object.

[c4] 4. The method of claim 1 further comprising

generating a key based upon the first portion and the second portion of the multi-token sealed object, and

obtaining the object of the multi-token sealed object by using the generated key to decrypt an encrypted object of the multi-token sealed object.

[c5] 5. The method of claim 1 further comprising

generating a key from the first portion and the second portion of the multi-token sealed object, and

obtaining the object of the multi-token sealed object by using the generated key and an a symmetric cryptographic algorithm to decrypt an encrypted object of the multi-token sealed object.

[c6] 6. The method of claim 1 further comprising

receiving a first key in response to the first token unsealing the sealed first portion,

receiving a second key in response to the second token unsealing the second portion,

generating a third key from the first key and the second key, and

obtaining the object of the multi-token sealed by using the third key to decrypt an encrypted object of the multi-token sealed object.

[c7] 7. The method of claim 1 further comprising

receiving a first key in response to the first token unsealing the sealed first portion only if the first token determines that a current device environment satisfies environment criteria specified for the sealed first portion,

receiving a second key in response to the second token unsealing the second portion only if the second token determines that the current device environment satisfies environment criteria specified for the sealed second portion,

generating a third key from the first key and the second key, and

obtaining the object of the multi-token sealed by using the third key to decrypt an encrypted object of the multi-token sealed object.

[c8] 8. The method of claim 7 further comprising

receiving the first key in response to the first token unsealing the sealed first portion only if a first value computed from the first portion and a first seal record of the sealed first portion has a predetermined relationship with a first digest value of the sealed first portion, and

receiving the second key in response to the second token unsealing the sealed second portion only if a second value computed from the second portion and a second seal record of the sealed second portion has a predetermined relationship with a second digest value of the sealed second portion.

[c9] 9. The method of claim 1 further comprising
receiving a first key in response to the first token unsealing the sealed first portion only if the first token generated the sealed first portion,
receiving a second key in response to the second token unsealing the second portion only if the second token generated the sealed second portion,
generating a third key from the first key and the second key, and
obtaining the object of the multi-token sealed by using the third key to decrypt an encrypted object of the multi-token sealed object.

[c10] 10. A method comprising
requesting a plurality of tokens to unseal a plurality sealed portions of a multi-token sealed object,
receiving a plurality of unsealed portions of the multi-token sealed object, and
obtaining an object that has been sealed to the plurality of tokens using the plurality of unsealed portions of the multi-token sealed object.

[c11] 11. The method of claim 10 wherein obtaining comprises
generating a key from the plurality of unsealed portions of the multi-token sealed object, and
decrypting an encrypted object using the key to obtain the object.

[c12] 12. The method of claim 10 wherein obtaining comprises
generating a key from the plurality of unsealed portions of the multi-token sealed object, and
decrypting an encrypted object using the key and a symmetric cryptographic algorithm to obtain the object.

[c13] 13. The method of claim 12 further comprising unsealing the plurality of sealed portions only if a current device environment satisfies device criteria specified for the plurality of sealed portions.

[c14] 14. The method of claim 12 further comprising unsealing the plurality of sealed portions only if the plurality of tokens generated the plurality of sealed portions.

[c15] 15. A method comprising
requesting a first token of a computing device to seal a first portion of a multi-token sealed object to first environment criteria, and
requesting a second token of a computing device to seal a second portion of the multi-token sealed object to second environment criteria.

[c16] 16. The method of claim 15 further comprising
encrypting an object using a symmetric cryptographic algorithm and a key to obtain an encrypted object, and
receiving a sealed encrypted object in response to the first token sealing the first portion that comprises the encrypted object,
receiving a sealed key in response to the second token sealing the second portion that comprises the key.

[c17] 17. The method of claim 15 further comprising
encrypting the object using an asymmetric cryptographic algorithm and an encryption key of an asymmetric key pair to obtain an encrypted object,
receiving a sealed encrypted object in response to the first token sealing the first portion that comprises the encrypted object,
receiving a sealed decryption key in response to the second token sealing the second portion that comprises a decryption key of the asymmetric key pair.

[c18] 18. The method of claim 15 further comprising
receiving a sealed first portion encrypted by the first token using a first key of the first token, the sealed first portion comprising the first key, a first seal record comprising one or more metrics specified by the first environment criteria, and a first digest value that attests to the integrity of the first key and the first seal record, and
receiving a sealed second portion encrypted by the second token using a second key of the second token, the sealed second portion comprising the second key, a second seal record comprising one or more metrics specified by the second environment criteria, and a second digest value that attests to the integrity of the second key and the second seal record.

[c19] 19. The method of claim 18 wherein
the first seal record comprises a unique first identifier for the first token, and
the second seal record comprises a unique second identifier for the second token.

[c20] 20. The method of claim 15 further comprising
encrypting the object using key that was generated based upon a first key and a second key,
receiving a sealed first key in response to the first token sealing the first portion that comprises the first key,
receiving a sealed second key in response to the second token sealing the second portion that comprises the second key.

[c21] 21. The method of claim 20 further comprising
generating a sealed first portion by encrypting the first portion and metrics specified by the first environment criteria using a first key of the first token, and
generating a sealed second portion by encrypting the second portion and metrics specified by the second environment criteria using a second key of the second token.

[c22] 22. The method of claim 21 wherein
the first token comprises a virtual token, and
the second token comprises a physical token.

[c23] 23. The method of claim 22 further comprising
specifying the second environment criteria by identifying at least one configuration register of the physical token that comprises a metric of the virtual token.

[c24] 24. The method of claim 15 further comprising
specifying the first environment criteria by identifying one or more configuration registers of the first token that record metrics of the computing device, and
specifying the second environment criteria by identifying one or more

configuration registers of the second token that record metrics of the computing device.

[c25] 25. The method of claim 24 wherein
specifying the second environment criteria comprises identifying at least one configuration register of the second token that comprises a metric of the first token.

[c26] 26. The method of claim 25 wherein
the first token comprises a virtual token, and
the second token comprises a physical token.

[c27] 27. A device comprising
a virtual token comprising one or more configuration registers that record metrics of a device environment and one or more processing units to generate a sealed first key that comprises a first key sealed to first environment criteria,
a physical token comprising one or more configuration registers that record metrics of the device environment, and one or more processing units to generate a sealed second key that comprises a second key sealed to second environment criteria, and
a sealing component to generate a third key based upon the first key and the second key, encrypt an object using the third key to obtain an encrypted object, request the virtual token to seal the first key to obtain the sealed first key, and request the physical token to seal the second key to obtain the sealed second key.

[c28] 28. The device of claim 27 wherein the sealing component specifies the first environment criteria by identifying one or more configuration registers of the virtual token to which to seal the first key, and specifies the second environment criteria by identifying one or more configuration registers of the physical token to which to seal the second key.

[c29] 29. The device of claim 28 wherein the sealing component specifies a first public key of the virtual token with which to seal the first key, and specifies a second public key of the physical token with which to seal the second key.

[c30] 30. The device of claim 29 wherein

the virtual token generates the sealed first key by using the first public key to encrypt the first key, a first seal record comprising metrics specified by the first environment criteria, and a first digest value that attests to the integrity of the first key and the first seal record, and

the physical token generates the sealed second key by using the second public key to encrypt the second key, a second seal record comprising metrics specified by the second environment criteria, and a second digest value that attests to the integrity of the second key and the second seal record.

[c31] 31. The device of claim 27 further comprising an unsealing component to request the virtual token to unseal the sealed first key to obtain the first key, to request the physical token to unseal the sealed second key to obtain the second key, to generate a third key based upon the first key and the second key, and to decrypt the encrypted object using the third key.

[c32] 32. The device of claim 31 wherein

the processing units of the virtual token further unseal the sealed first key and provide the unsealing component with the first key only if the metrics of the one or more configuration registers of the virtual token satisfy the first environment criteria, and

the processing units of the physical token further unseal the sealed key and provide the unsealing with the key used to decrypt the encrypted object only if the metrics of the one or more configuration registers of the physical token satisfy the second environment criteria.

[c33] 33. The device of claim 32 wherein

the virtual token unseals the sealed object by decrypting the sealed object using a first private key of the virtual token to obtain the encrypted object, a first seal record, and a first digest value that attests to the integrity of the encrypted object and the first seal record, and

the physical token unseals the sealed key by decrypting the sealed key using a second private key of the physical token to obtain the key, a second seal record, and a second digest value that attests to the integrity of the key and

the second seal record.

[c34] 34. The device of claim 31 wherein
the processing units of the virtual token provide the unsealing component with the encrypted object only if the first digest value obtained from the sealed first key has a predetermined relationship with a value computed from the first key and the first seal record of the sealed first key, and
the processing units of the physical token provide the unsealing component with the second key only if the second digest value obtained from the sealed second key has a predetermined relationship with a value computed from the second key and the second seal record of the sealed second key.

[c35] 35. A machine readable medium comprising a plurality of instructions that, in response to being executed, result in a computing device
sealing a first portion of a multi-token sealed object to first environment criteria using a first public key of a first token to obtain a sealed first portion, and
sealing a second portion of the multi-token sealed object to second environment criteria using a second public key of a second token to obtain a sealed second portion.

[c36] 36. The machine readable medium of claim 35 wherein the plurality of instructions further result in the computing device
specifying the first environment criteria by identifying one or more configuration registers of the first token that record metrics of the computing device, and
specifying the second environment criteria by identifying one or more configuration registers of the second token that record metrics of the computing device.

[c37] 37. The machine readable medium of claim 36 wherein the plurality of instructions further result in the computing device
generating the sealed first portion such that the sealed first portion comprises the first portion, a first seal record comprising the metrics of the one or more configuration registers specified by the first environment

criteria, and a first digest value of the encrypted object and the seal record, and

generating the sealed second portion such that the sealed second portion comprises the second portion, a second seal record comprising the metrics of the one or more configuration registers specified by the second environment criteria, and a second digest value of the key and the second seal record.

[c38] 38. The machine readable medium of claim 37 wherein the plurality of instructions further result in the computing device

unsealing the sealed first portion using a first private key of the first token and providing the first portion only if the metrics recorded by the first token have a predetermined relationship with the metrics of the first seal record, and

unsealing the sealed second portion using a second private key of the second token and providing the second portion only if the metrics recorded by the second token have a predetermined relationship with the metrics of the second seal record.

[c39] 39. The machine readable medium of claim 38 wherein the plurality of instructions further result in the computing device

providing the first portion only if the first digest value obtained from the sealed encrypted object has a predetermined relationship to a first value computed from the encrypted object and the first seal record, and

providing the second portion only if the second digest value obtained from the sealed key has a predetermined relationship to a second value computed from the key and the second seal record.

[c40] 40. The machine readable medium of claim 35 wherein the plurality of instructions further result in the computing device

unsealing the sealed first portion using a first private key of the first token and providing the first portion object only if a current device environment satisfies the first environment criteria, and

unsealing the sealed second portion using a second private key of the second token and providing the second portion only if the current device environment satisfies the second environment criteria.

[c41] 41. A device comprising

a chipset,

a processor coupled to the chipset,

memory coupled to the chipset, the memory comprising a plurality of instructions that, when executed by the processor, result in the processor implementing a virtual token that records metrics of a device environment, that receives a first key used to generate a decryption key, and that seals the first key to one or more metrics recorded by the virtual token in response to receiving a seal operation request, and

a physical token coupled to the chipset, the physical token to record metrics of the device environment, to receive a second key used to generate the decryption key, and to seal the second key to one or more metrics recorded by the physical token in response to receiving a seal operation request.

[c42] 42. The device of claim 41 wherein the one or more metrics recorded by the physical token comprises a virtual token metric and the physical token seals the key to at least the virtual token metric.

[c43] 43. The device of claim 41 wherein the one or more metrics recorded by the physical token comprises a metric of the plurality of instructions that result in the processor implementing the virtual token and the physical token seals the key to at least the metric of the plurality of instructions.

[c44] 44. The device of claim 41 wherein

the plurality of instructions, in response to execution, result in the processor generating a sealed first key that comprises the first key and a unique first identifier for the virtual token, and

the physical token generates a sealed second key that comprises the second key and a unique second identifier for the physical token.